

REMARKS

This Application has been carefully reviewed in light of the Office Action mailed April 26, 2006 ("Office Action"). At the time of the Office Action, Claims 1-71 were pending and Claims 1-26, 35-41, 50-56, and 65-71 were withdrawn. The Examiner rejects Claims 27-34, 42-49, and 57-64. Applicant amends Claims 27, 42, and 57. As described below, Applicant believes all claims to be allowable over the cited references. Therefore, Applicant respectfully requests reconsideration and full allowance of all pending claims.

Section 112 Rejections

The Examiner rejects Claims 27, 42, and 57 under 35 U.S.C. § 112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. Specifically, the Examiner states that "there is no connection between pre-set list of hostile applications with other claim limitations." (Office Action, pages 3-4). Although Applicant believes that the claims as written did not omit essential steps, Applicant has amended Claims 27, 42, and 57. Applicant submits that Claims 27, 42, and 57, as amended, are in accordance with 35 U.S.C. § 112, second paragraph. Therefore, Applicant respectfully requests reconsideration and allowance of Claims 27, 42, 57, together with Claims 28-34, 43-49, and 58-64 which depend respectively therefrom.

Section 103 Rejections

The Examiner rejects Claims 27-32, 34, 42-47, 49, 57-62, and 64 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,092,194 issued to Touboul ("*Touboul*") in view of U.S. Patent No. 5,859,966 issued to Hayman et al. ("*Hayman*"). The Examiner rejects Claims 33, 48, and 63 under 35 U.S.C. § 103(a) as being unpatentable over *Touboul* in view *Hayman* and further in view of U.S. Patent No. 5,987,523 issued to Hind et al. ("*Hind*"). For the reasons discussed below, Applicant respectfully requests reconsideration and allowance of Claims 27-34, 42-49, and 57-64.

1. The Claims are Allowable over the Cited References

Independent Claim 27 of the present Application, as amended, recites:

A method for preventing hostile use of computer resources by an application running on a workstation, comprising:

providing, on a workstation, a pre-set list of applications permitted to run on the workstation and a list of one or more computer resources on the workstation to which are not accessible to unspecified applications;

providing a filter on a workstation for receiving internal requests for computer resources resident on the workstation;

receiving at the filter a request for access generated by an unspecified application downloaded to the workstation from a source external to the workstation, the request for access identifying a computer resource resident on the workstation to which the unspecified application seeks access;

determining that the unspecified application is not identifiable in the pre-set list of hostile applications;

in response to determining that the unspecified application is not identifiable in the pre-set list of hostile applications, determining whether the requested computer resource is on the list of one or more computer resources that are not accessible to unspecified applications;

allowing access to the requested computer resource if the requested computer resource is not on the list of one or more computer resources; and

preventing access to the requested computer resource if the requested computer resource is on the list of one or more computer resources.

Applicant respectfully submits that the proposed *Touboul-Hayman* combination, as relied upon by the Examiner in the Office Action, does not disclose, teach, or suggest the combination of features and operations recited in Applicants' Claim 27.

For example, Applicant respectfully submits that the proposed *Touboul-Hayman* combination does not disclose, teach, or suggest "providing, on a workstation, a pre-set list of applications permitted to run on the workstation and a list of one or more computer resources on the workstation to which are not accessible to unspecified applications," as recited in Applicant's Claim 27. As previously noted by Applicant, *Touboul* relates to an "internal network security system 110 [that] examines Downloadables received from external computer network 105, and prevents Downloadables deemed suspicious from reaching the internal computer network." (Column 3, lines 9-12). Thus, *Touboul* is a network based application designed to prevent hostile Downloadables from breaching the internal network. Thus, there can be no disclosure by *Touboul* of "providing, on a workstation, a preset list of applications . . . and a list of one or more computer resources on the workstation," as recited in Claim 27. Furthermore, *Touboul* merely discloses that security policies may "identify specific Downloadables to block, specific Downloadables to allow, or necessary criteria for

allowing an unknown Downloadable.” (Column 4, lines 20-23). *Touboul* does not disclose, teach, or suggest using “a list of one or more computer resources on the workstation to which are not accessible to unspecified applications,” as recited in Claim 27.

Applicants further submit that these deficiencies are not cured by the disclosure of *Hayman*. To the contrary, *Hayman* discloses “a security system for a computer system in which specific limitations are imposed on who has access to exactly what computer functions and data on the computer system.” (Column 1, lines 48-51). Accordingly, the *Hayman* system determines the permissibility of user-requested computer functions on a user-by-user basis. With regard to viruses, *Hayman* further discloses that “viruses are securely contained and prevented from expanding.” (Column 1, lines 53-55). Specifically, “[w]hen a process runs a program, a copy of the program is made into memory allocated to that process.” (Column 7, lines 23-25). “If the program contains malicious code which attempts to modify any objects in the virus prevention region (where all system executables and many other system files are placed), access will be denied.” (Column 7, lines 25-28). Thus, *Hayman* merely discloses that objects in certain region of the computer system may not be modified by malicious code. Accordingly, *Hayman* also does not disclose, teach, or suggest “providing, on a workstation, a pre-set list of applications permitted to run on the workstation and a list of one or more computer resources on the workstation to which are not accessible to unspecified applications,” as recited in Applicant’s Claim 27.

As still another example, Applicant respectfully submits that the proposed *Touboul-Hayman* combination does not disclose, teach, or suggest “determining that the unspecified application is not identifiable in the pre-set list of hostile applications” and “in response to determining that the unspecified application is not identifiable in the pre-set list of hostile applications, determining whether the requested computer resource is on the list of one or more computer resources that are not accessible to unspecified applications,” as recited in Applicant’s Claim 27. As previously discussed, *Touboul* merely discloses that security policies may “identify specific Downloadables to block, specific Downloadables to allow, or necessary criteria for allowing an unknown Downloadable.” (Column 4, lines 20-23). The process is described with regard to Figure 6A. Specifically, “the first comparator 320 in step 608 examines the lists of Downloadables to allow or to block per administrative override 425

against the Downloadable ID of the incoming Downloadable to determine whether to allow the Downloadable automatically.” (Column 7, lines 60-64). If it is not allowed automatically, “the first comparator 620 examines the lists of Downloadables to block per administrative override 425 against the Downloadable ID of the incoming Downloadable for determining whether to block the Downloadable automatically.” (Column 7, line 66 through Column 8, line 3). If the Downloadable is not blocked automatically, a “URL comparator 350” may compare “the URL embodied in the incoming Downloadable against the URLs of the URL rules bases 420.” (Column 8, lines 9-13). Alternatively, DSP data may be examined “to determine whether the Downloadable has been previously decomposed.” (Column 8, lines 16-20). As still another alternative, a certificate scanner may “scan the Downloadable for an embodied certificate” and a certificate comparator may “[retrieve] trusted certificates from the trusted certificate lists (TCL) 415 and [compare] the embodied certificate with the trusted certificates to determine whether the Downloadable has been signed by a trusted source.” (Column 8, lines 33-39). None of the steps or combination of steps described in *Touboul*, however, are analogous to both “determining that the unspecified application is not identifiable in the pre-set list of hostile applications” and “in response to determining that the unspecified^{*} application is not identifiable in the pre-set list of hostile applications, determining whether the requested computer resource is on the list of one or more computer resources that are not accessible to unspecified applications,” as recited in Applicant’s Claim 27.

These deficiencies also are not cured by the disclosure of *Hayman*. To the contrary, *Hayman* discloses “a security system for a computer system in which specific limitations are imposed on who has access to exactly what computer functions and data on the computer system.” (Column 1, lines 48-51). As described previously, *Hayman* discloses, with regard to viruses, that “[w]hen a process runs a program, a copy of the program is made into memory allocated to that process.” (Column 7, lines 23-25). “If the program contains malicious code which attempts to modify any objects in the virus prevention region (where all system executables and many other system files are placed), access will be denied.” (Column 7, lines 25-28). Thus, *Hayman* merely discloses that objects in certain regions of the computer system may not be modified by malicious code. Accordingly, *Hayman* also does not disclose, teach, or suggest “determining that the unspecified application is not

identifiable in the pre-set list of hostile applications” and “in response to determining that the unspecified application is not identifiable in the pre-set list of hostile applications, determining whether the requested computer resource is on the list of one or more computer resources that are not accessible to unspecified applications,” as recited in Applicant’s Claim 27.

For at least these reasons, Applicants respectfully request reconsideration and allowance of Claim 27, together with Claims 28-34 that depend from Claim 27.

Independent Claims 42 and 57 recite certain features that are analogous to those discussed above. For example, Claim 42 recites “a processor . . . operable to . . . maintain a pre-set list of applications permitted to run on the workstation and a list of one or more computer resources on the workstation that are not accessible to any unspecified applications.” Claim 42 also recites that “in response to a request received from the unspecified application,” the processor is operable to “determine that the unspecified application is not identifiable in the pre-set list of applications.” Claim 42 further recites “in response to determining that the unspecified application is not identifiable in the pre-set list of applications,” the processor is operable to “determine whether a requested computer resource is on the list of one or more computer resources on the workstation that are not accessible to any unspecified applications.” Claim 57 recites logic operable when executed to “maintain, on a workstation, a pre-set list of applications permitted to run on the workstation and a list of one or more computer resources on the workstation to which are not accessible to unspecified applications.” The logic of Claim 57 is also operable to “determine that the unspecified application is not identifiable in the pre-set list of applications permitted to run on the workstation” and “in response to determining that the unspecified application is not identifiable in the pre-set list of applications, determine whether the requested computer resource is on the list of one or more computer resources that are not accessible to unspecified applications.” Accordingly, for reasons similar to those discussed above, Applicants respectfully submit that the proposed *Touboul-Hayman* combination does not disclose, teach, or suggest each and every limitation of Applicants’ Claims 42 and 57.

For at least these reasons, Applicants respectfully request reconsideration and allowance of Claims 42 and 57, together with Claims 43-49 and 58-64 that depend from Claims 42 and 57, respectively.

2. The Proposed *Touboul-Hayman* and *Touboul-Hayman-Hind* Combinations are Improper

Assuming for purposes of argument only that the proposed combinations discloses the limitations of Applicants' Claims 27-71 (which Applicants dispute above), the Examiner has not cited language in either reference or within information commonly known to those skilled in the art that provides the necessary motivation or suggestion to combine *Touboul* and *Hayman*. Additionally, one of ordinary skill in the art would not have been motivated to make the proposed combination.

The M.P.E.P. sets forth the strict legal standard for establishing a *prima facie* case of obviousness based on modification or combination of prior art references. "To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references where combined) must teach or suggest all the claim limitations." M.P.E.P. § 2142, 2143. The teaching, suggestion or motivation for the modification or combination and the reasonable expectation of success must both be found in the prior art and cannot be based on an Applicant's disclosure. *See Id.* (citations omitted). "Obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either explicitly or implicitly in the references themselves or in the knowledge generally available to one of ordinary skill in the art" at the time of the invention. M.P.E.P. § 2143.01. Even the fact that references *can* be modified or combined does not render the resultant modification or combination obvious unless the prior art teaches or suggests the desirability of the modification or combination. *See Id.* (citations omitted).

The governing Federal Circuit case law makes this strict legal standard even more clear.¹ According to the Federal Circuit, “a showing of a suggestion, teaching, or motivation to combine or modify prior art references is an essential component of an obviousness holding.” *In re Sang-Su Lee*, 277 F.3d 1338, 1343, 61 U.S.P.Q.2d 1430, 1433 (Fed. Cir. 2002) (quoting *Brown & Williamson Tobacco Corp. v. Philip Morris Inc.*, 229 F.3d 1120, 1124-25, 56 U.S.P.Q.2d 1456, 1459 (Fed. Cir. 2000)). “Evidence of a suggestion, teaching, or motivation . . . may flow from the prior art references themselves, the knowledge of one of ordinary skill in the art, or, in some cases, the nature of the problem to be solved.” *In re Dembiczak*, 175 F.3d 994, 999, 50 U.S.P.Q.2d 1614, 1617 (Fed. Cir. 1999). However, the “range of sources available . . . does not diminish the requirement for actual evidence.” *Id.* Even a determination that it would have been obvious to one of ordinary skill in the art at the time of the invention to try the proposed modification or combination is not sufficient to establish a *prima facie* case of obviousness. *See In re Fine*, 837 F.2d 1071, 1075, 5 U.S.P.Q.2d 1596, 1599 (Fed. Cir. 1988).

In addition, the M.P.E.P. and the Federal Circuit repeatedly warn against using an applicant’s disclosure as a blueprint to reconstruct the claimed invention. For example, the M.P.E.P. states, “The tendency to resort to ‘hindsight’ based upon applicant’s disclosure is often difficult to avoid due to the very nature of the examination process. However, impermissible hindsight must be avoided and the legal conclusion must be reached on the basis of the facts gleaned from the prior art.” M.P.E.P. § 2142. The governing Federal Circuit cases are equally clear. “A critical step in analyzing the patentability of claims pursuant to [35 U.S.C. § 103] is casting the mind back to the time of invention, to consider the thinking of one of ordinary skill in the art, guided only by the prior art references and the then-accepted wisdom in the field. . . . Close adherence to this methodology is especially important in cases where the very ease with which the invention can be understood may prompt one ‘to fall victim to the insidious effect of a hindsight syndrome wherein that which only the invention taught is used against its teacher.’” *In re Kotzab*, 217 F.3d 1365, 1369, 55 U.S.P.Q.2d 1313, 1316 (Fed. Cir. 2000) (citations omitted). In *In re Kotzab*, the Federal Circuit noted that to prevent the use of hindsight based on the invention to defeat

¹ Note M.P.E.P. 2145 X.C. (“The Federal Circuit has produced a number of decisions overturning obviousness rejections due to a lack of suggestion in the prior art of the desirability of combining references.”).

patentability of the invention, the court requires the Examiner to show a motivation to combine the references that create the case of obviousness. *See id.* *See also, e.g., Grain Processing Corp. v. American Maize-Products*, 840 F.2d 902, 907, 5 U.S.P.Q.2d 1788, 1792 (Fed. Cir. 1988). Similarly, in *In re Dembiczak*, the Federal Circuit reversed a finding of obviousness by the Board, explaining that the required evidence of such a teaching, suggestion, or motivation is essential to avoid impermissible hindsight reconstruction of an applicant's invention:

Our case law makes clear that the best defense against the subtle but powerful attraction of hind-sight obviousness analysis is *rigorous application of the requirement for a showing of the teaching or motivation to combine prior art references*. Combining prior art references without evidence of such a suggestion, teaching, or motivation simply takes the inventor's disclosure as a blueprint for piecing together the prior art to defeat patentability—the essence of hindsight.

175 F.3d at 999, 50 U.S.P.Q.2d at 1617 (emphasis added) (citations omitted).

With respect to Applicant's independent claims, the Examiner acknowledges that *Touboul* does not disclose "when unspecified application runs on the workstation, preventing the application from accessing any resource directly." (Office Action, page 5). The Examiner speculates, however, that "it would have been obvious . . . to employ the use of preventing unspecified application from accessing any resource directly in the system of *Touboul* as *Hayman* teaches to effectively protect computer resources." (Office Action, page 5). Applicants respectfully submit that the Examiner's summary conclusion amounts to mere speculation and does not provide the suggestion or motivation necessary to make the proposed combination.² The mere possibility that the security system of *Hayman* might improve the system of *Touboul*, as the Examiner asserts, does not even remotely provide the required teaching, suggestion, or motivation to modify the teachings of *Touboul*. Applicants respectfully submit that in making this unobvious leap the Examiner has used the type of hindsight reconstruction explicitly forbidden by the M.P.E.P. and Federal Circuit.

² If the Examiner is relying on "common knowledge" or "well known" art in support of his rationale for combining *Touboul* and *Hayman*, the Examiner is requested to produce a reference in support of his position pursuant to M.P.E.P. § 2144.03. If the Examiner is relying on personal knowledge to supply the required motivation or suggestion to combine *Touboul* and *Hayman*, Applicants respectfully request that the Examiner produce an affidavit supporting such facts pursuant to M.P.E.P. § 2144.03.

Furthermore, Applicants respectfully submit that one of ordinary skill in the art at the time of Applicants' invention would not have been motivated to make the proposed *Touboul-Hayman* combination. Applicants acknowledge that *Touboul* and *Hayman* relate generally to security systems. Applicants respectfully submit, however, that this is both the beginning and ending of any similarity between the two references. Whereas *Touboul* relates to a network-based application that prevents hostile applications from breaching an internal network (Column 3, lines 9-12), *Hayman* relates to determining the permissibility of user-requested computer functions on a user-by-user basis. (Column 1, line 48 through Column 2, lines 2-4). Thus, the solution proposed by *Hayman* (restricting access to files "so that only users who possess certain privileges can access to the file") is designed to prevent all users from having total access to the system. This is entirely different and unrelated to the solution proposed by *Touboul* (preventing hostile applications from reaching network devices). Furthermore, there is no explicit or implicit reference in either reference which would suggest to one of ordinary skill to combine the network-based security system of *Touboul* with the user-based system of *Hayman*. In this respect, Applicants respectfully submit that the references are non-analogous art and, because not related, an improper combination.

In the Office Action, the Examiner states that *Touboul* "not only discloses a network-based application preventing hostile applications from breaching an internal network but also discloses security policies applied to client or group to which client belongs (col. 2, lines 1-6). (Office Action, page 3). The portion cited by the Examiner, however, merely states that "the security policy may include a default security policy to be applied regardless of the client to whom the Downloadable is addressed, a specific security policy to be applied based on the client or the group to which the client belongs, or a specific policy to be applied based on the client/group and on the particular Downloadable received." (Column 1, line 67 through Column 2, line 6). Thus, the relied upon portion merely states that the security policy may be tailored to the entire group of clients in the network or to a group of clients in the network. The relied upon portion does not change the fact that the objective of *Touboul* is to provide a network solution to prevent hostile Downloadables from breaching the network - an objective that is entirely different from the user-based system of *Hayman*.

For at least these reasons, Applicants respectfully submit that the proposed *Touboul-Hayman* combination is improper.

CONCLUSION

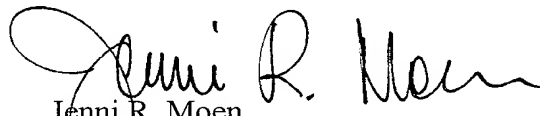
Applicants have made an earnest attempt to place this case in condition for allowance. For the foregoing reasons, and for other reasons clearly apparent, Applicants respectfully request full allowance of all pending claims.

No fee is believed to be due. However, the Commissioner is hereby authorized to charge any fees or credit any overpayment to Deposit Account No. 02-0384 of Baker Botts L.L.P.

If there are matters that can be discussed by telephone to further the prosecution of this application, Applicants respectfully request that the Examiner call its attorney at the number listed below.

Respectfully submitted,

BAKER BOTTS L.L.P.
Attorneys for Applicants


Jenni R. Moen
Reg. No. 52,038
(214) 953-6809

Date: August 24, 2006

CORRESPONDENCE ADDRESS:

Customer No.: **05073**